DETAILED ACTION

1. The "FINAL ACTION" mailed 2/04/09 did not appropriately indicate that the action was final. Therefore, the Advisory Action issued on 5/26/2009 is withdrawn. This action is in response to the amendment filed 5/18/2009. Claims 38 and 49 are amended. Claim 44 is cancelled. Claims 1, 2, 3, 5, 7 - 25, 27, 29 43 and 45- 61 are pending.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

2. Claims 38 and 49 rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. The Examiner contends applicant's newly amended subject matter of "said open portion is the portion containing data unauthorized modification of which may not cause an impostor to be incorrectly authenticated as a genuine user and comprises parameters of a predetermined number of unique features of the biometric identification template", lacks support of original disclosure.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claims 1-3, 5, 7-25, 27, and 29-37 are rejected under 35 U.S.C. 102(e) as being anticipated by Hamid (US Patent No. 2003/0223624).

4. As to claim 1, Hamid teaches a method of authenticating a user according to a biometrics parameter of the user presented at an authentication device on a user-presented device on which is stored a biometrics identification template (i.e., fingerprint template) divided into a secure portion (e.g., private portion) and an open portion (e.g., public portion) [par. 27],

the method comprising: transmitting to a client terminal (i.e., smart card reader interface) data derived from said user biometrics parameter at the authentication device [par. 27], wherein the open portion (e.g., public portion) is the portion containing data unauthorized modification of which may not cause an impostor to be incorrectly authenticated as a genuine user and comprises parameters of a predetermined number of unique features of the template [par. 27];

transmitting from a user-presented device (i.e., smart card) to the client terminal only the open portion (e.g., public portion) of the said biometrics identification template held on the user-presented device (e.g., smart card) (i.e., ... Hamid teaches transmitting from a smart card a public portion to a host computer [par. 27], a open portion is the portion containing data unauthorized modification of which may not cause an impostor to be incorrectly authenticated as a genuine user and comprises parameters of a predetermined number of unique features of the template and user-presented device (e.g., ... teaches providing a public portion from a smart card for which is preprocessed registered biometric data [par. 26-27]). at the client terminal (e.g., host processor) implementing a first stage of an biometric identity authentication process between said derived data and said open portion to produce intermediate results and transmitting the intermediate results of said biometric authentication process to the user-presented device (i.e., ... teaches a host processor align sensed image with portion of fingerprint received. Extracting the aligned image and creating a image portion [26, 27, fig. 3]), wherein said intermediate results (e.g., image portion) comprise parameters for alignment of said derived data and said biometric identification template (i.e., ... teaches providing a image portion extracted from an aligned image from which a derived private portion was constructed [par. 27]); and at the user-presented device (i.e., smart card) implementing a second stage of the biometric identity authentication process to complete the biometric identity authentication process using said intermediate results and issuing a biometric authentication result based thereon (e.g., ... teaches a smart card comparing a image portion with a private portion [29, fig. 3]).

5. As to claim 2, Hamid teaches a method of registration of a user according to a biometrics parameter of the user presented at an authentication device [par. 26], the method comprising; transmitting to an authorized client terminal) data said user biometrics parameter obtained at the authentication device [par. 26]; at the authorized client terminal, dividing the biometrics identification template computed into secure portion and open portion [par. 26],

a open portion is the portion containing data unauthorized modification of which may not cause an impostor to be incorrectly authenticated as a genuine user and comprises parameters of a predetermined number of unique features of the template (i.e., ... teaches providing a public portion from a smart card for which is preprocessed registered biometric data [par. 26-27]; transmitting from the authorized client terminal (e.g., imaging device), to a user-presented device both the open portion and the secure portion of a biometrics identification template [par. 26], storing the said template consisting of open and secure portions on the user- presented device [par. 26].

6. As to claim 3, Hamid teaches a method where the secure portion of the biometrics identification template is the portion containing data unauthorized modification of which may cause an impostor to be incorrectly authenticated as a genuine user (i.e., Burger teaches user biometric characteristics stored on a portable standalone device [fig. 1]).

7. As to claim 4, Cancelled.

8. As to claim 5, Hamid teaches a method where the biometrics parameter is a Fingerprint (103, 104, fig. 4).

9. As to claim 6, Cancelled.

10. As to claim 7, Hamid teaches a method where the first stage of said biometric identity authentication process implemented at the client terminal comprises locating unique features using the data derived from the user biometrics parameter and aligning them with said predetermined number of unique features from the identification template held on the user-presented device (106, fig. 4).

11. As to claim 8, Hamid teaches a method where the second stage of the said identity authentication process implemented on the user-presented device (i.e., smart card) is implemented using a local executable matching program (i.e., application) stored on the device (109, 110, fig, 4).

12. As to claim 9, Hamid teaches a method where the first stage of the identity authentication process implemented at the client terminal is implemented using a client executable matching program (106, 107, fig. 4).

13. As to claim 10, Hamid teaches a method where the client executable matching program is stored on the user-presented device (i.e., smart card) or the authentication device and is transmitted to the client terminal at the time of authentication [par. 23].

14. As to claim 11, Hamid teaches a method where the client executable matching program (i.e., biometric template) is downloaded by the client terminal from a remote memory (i.e., smart card) at the time of authentication [par. 23].

15. As to claim 12, Hamid teaches a method where the authentication result is used to authenticate a user for authorizing a secure transaction [par. 25].

16. As to claim 13, Hamid teaches a method where the secure transaction is controlled by an executable transaction program stored on the user-presented device [par. 64].

17. As to claim 14, Hamid teaches a method where when the authentication result indicates an adequate match, a first security access check key (e.g., image portion) is constructed including the authentication result [26, fig. 3]

18. As to claim 15, Hamid teaches a method where a second security access check key is requested and compared with the first security access key (e.g., image portion),

the result of said comparison being used to enable the executable transaction program if it yields a positive authentication result [28, 29, fig. 3].

19. As to claim 16, Hamid teaches a method where the second security access check key (e.g., image portion) is issued from a security server [28, fig. 3].

20. As to claim 17, Hamid teaches a method where the first and second security access check keys each include a unique identification number [24, fig. 3].

21. As to claim 18, Hamid teaches a method where the unique identification number contains a number obtained from a mathematical operation on a randomly generated number and the authentication result [par. 48].

22. As to claim 19, Hamid teaches a method where the randomly generated number changes at each time the number is used [par. 55].

23. As to claim 20, Hamid teaches a method where the changing random number is tracked by dividing the number into two portions, a first portion to be used as the current random number and a second portion to be used as the next random number [par. 47].

24. As to claim 21, Hamid teaches a method where the unique identification number contains a number that is remembered by the user [par. 27]. 22. As to claim 22, Hamid

teaches a method where more than one authentication methods can be used to obtain the authentication result, each being incorporated into the unique identification number (par. 27).

25. As to claim 23, Hamid teaches a method where the access is divided into several levels and wherein the level of access granted to a user is dependent on the confidence level of positive identity obtained from the unique identification number (i.e., ... teaches a multiple security level using PIN and biometric authentication [par. 27]).

26. As to claim 24, Hamid teaches a system for authenticating a user according to a biometrics parameter of the user, the system comprising: a user-presented device (i.e., smart card) on which is stored a biometrics identification template divided into a secure portion and an open portion [par. 26], where only said open portion can be transmitted out of the said device; an authentication device (i.e., smart card reader interface) operable to read biometrics data derived from a user [25, fig. 3], where only said open portion is the portion containing data unauthorized modification of which may not cause an impostor to be incorrectly authenticated as a genuine user and comprises parameters of a predetermined number of unique features of the template (i.e., ... teaches providing a public portion from a smart card for which is preprocessed registered biometric data [par. 26-27]),

an authentication device operable to read biometric data derived from a user [par. 27], and comprising means for communicating with the user-presented device and

a client terminal (par. 23) a client terminal arranged to receive the said open portion of the biometrics identification template held on the user-presented device (i.e., smart card) and the biometrics data derived from the user, and comprising a client processor operable to implement a first stage of biometric identity authentication process between said derived data and said open portion to produce intermediate results [par. 27], and to transmit the intermediate results of said biometric identity authentication process to the user-presented device [28, fig. 3], wherein said intermediate results (e.g., image portion) comprise parameters for alignment of said derived data and said biometric identification template (i.e., ... teaches a providing a image portion extracted from an aligned image from which a derived private portion was constructed [par. 27]);

and wherein the user-presented device (i.e., smart card) comprises a device processor operable to implement a second stage of the biometric identity authentication process to complete the biometric identity authentication process using said intermediate results and to issue a biometric authentication result based thereon (to provide a smart card biometric authentication capability [col. 7, lines 60-67]).

27. As to claim 25, Hamid teaches a system where the secure portion of the biometrics identification template is the portion containing data unauthorized modification of which may cause the system to incorrectly authenticate an impostor as a genuine user [par. 23]

28. As to claim 26, Cancelled

29. As to claim 27, Hamid teaches a system where the biometrics parameter is a fingerprint, and where the authentication device includes a fingerprint Sensor (par. 23).

30. As to claim 28, Cancelled.

31. As to claim 29, Hamid teaches a system where the user-presented device (i.e., smart card) comprises a memory (i.e., micro chip) in which is stored a local executable matching program (i.e., application) for implementing the second stage of the matching process [par. 64].

32. As to claim 30, Hamid teaches a system where the memory on the user-presented device stores a client executable matching program which is transmitted to the client processor to implement the first stage of the matching process (par. 23).

33. As to claim 31, Hamid teaches a system which comprises a security server connected to the client terminal [par. 64].

34. As to claim 32, Hamid, teaches a system where the security server (i.e., host processor) holds a client executable matching program for implementing the first stage of the matching process [par. 23].

35. As to claim 33, Hamid teaches a system where the security server holds a security access check key requestable (e.g., biometric sample) by the client terminal for enabling a transaction [par. 64].

36. As to claim 34, Hamid teaches a system which comprises a transaction server arranged to implement secure transactions and which is in communication with the client terminal so that the authentication result is usable to authenticate a user for authorizing a secure transaction [par. 25].

37. As to claim 35, Hamid teaches a system where the user-presented device stores an executable transaction program (i.e., biometric data) for controlling the secure transaction (par. 64).

38. As to claim 36, Hamid teaches a system where more than one authentication methods can be used to obtain the authentication result (par. 27)

39. As to claim 37, Hamid teaches a system where the access to the transaction server is divided into several levels and wherein the level of access granted to a user is dependent on the confidence level of positive identity obtained based on the results from the various authentication methods used (par. 27).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

40. Claims 38-43, 45-61 are rejected under 35 U.S.C. 103(a) as being unpatentable over Studd in view of Hamid.

41. As to claim 38, Studd teaches a method of executing an operation using first and second processors, the method comprising: storing in the first processor a first task table containing a plurality of process names (i.e., mobile device application) with associated process identifiers, each associated with a process locator (i.e., Studd

teaches a request for a list of mobile device application from mobile to device for which said mobile device application will be stored and executed [par. 51]);

storing in the second processor a second task table containing said of process names and process identifiers (i.e., Studd teaches a mobile device containing list mobile device application [par. 51]);

identifying at the second processor a process to be executed and issuing a request to the first processor to execute said process (i.e., Studd teaches identifying a mobile application to execute [par. 51 - par. 53]); locating said process using the process locator and executing said process at the first processor to generate a result [par. 51 - par. 53]; and returning the result to the second processor [par. 51 - par. 53].

Studd does not expressly teach:

wherein the operation being executed is a fingerprint- matching algorithm comprising a base minutiae finding process executed by the first processor and a minutiae matching process executed by the second processor, wherein the base minutiae finding process is a first stage of a biometric identity authentication process implemented between data derived from a user biometric parameter and an open portion of a biometric identification template to produce intermediate results,

said open portion is the portion containing data unauthorized modification of which may not cause an impostor to be incorrectly authenticated as a genuine user and comprises parameters of a predetermined number of unique features of the biometric identification template, and said intermediate results comprise parameters for alignment

of said data and said biometric identification template and are transmitted from the first processor to the second processor, and wherein the minutiae matching process is a second stage of the biometric identity authentication process to issue a biometric authentication result using the intermediate results.

However, these features are well known in the art and would have been an obvious modification of the system disclosed by Studd as introduced by Hamid. Hamid discloses:

wherein the operation being executed is a fingerprint- matching algorithm comprising a base minutiae finding process executed by the first processor and a minutiae matching process executed by the second processor (to provide a fingerprint minutiae matching algorithm [col. 7, lines 20- 51]).

wherein the base minutiae finding process is a first stage of a biometric identity authentication process implemented between data derived from a user biometric parameter and an open portion of a biometric identification template to produce intermediate results (to provide a transmitting capability from a smart card a public portion (e.g., open) to a host computer for the purpose of authentication [par. 27],

said open portion is the portion containing data unauthorized modification of which may not cause an impostor to be incorrectly authenticated as a genuine user and comprises parameters of a predetermined number of unique features of the biometric identification template (to provide a public portion (e.g. open) containing authentication data [par. 27]),

and said intermediate results comprise parameters for alignment of said data and said biometric identification template and are transmitted from the first processor to the second processor, and wherein the minutiae matching process is a second stage of the biometric identity authentication process to issue a biometric authentication result using the intermediate results (to provide processing at the host for biometric authentication [26, 27, fig. 3]].

Therefore, given the teachings of Hamid, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Studd by employing the well known features of a fingerprint matching algorithm disclosed above by Hamid, for which distributed authentication will be enhanced [col. 7, lines 20-51].

42. As to claim 39, Studd teaches a method where said process names (i.e., identifiers) include object names associated with respective object identifiers [par. 51, lines 7-10].

43. As to claim 40, Studd teaches a method where each object has associated therewith a plurality of functions (i.e., mobile device application) each identified by function names and associated function identifiers in the first and second task tables (par. 51).

44. As to claim 41, Studd teaches a method where the process locator identifies (i.e., identifier) the starting address of a process in a program memory (par. 51, lines 7-10).

45. As to claim 42, Studd teaches a method where the second processor has significantly less processing power than the first processor (par. 29, lines 8-11).

46. As to claim 43, Studd teaches a method where the second processor is arranged to execute locally processes requiring less processing power than those executed by the first processor [fig. 5].

47. As to claim 45, Studd teaches a method where there are a plurality of second processors in communication with a single first processor, each second processor holding a respective task table, and the first processor holding a first task table (i.e., mobile device application) including all processes identified by the task tables of the second processors (i.e., Studd teaches a mobile device with a list of mobile device applications [par. 50- par. 53]).

48. As to claim 46, Studd teaches a method where a client bridge (i.e., predetermine mechanism) is connected between the first and second processors, the client bridge (i.e., predetermine mechanism) conveying said requests from the second processor to the first processor and returning the results from the first processor to the second processor (par. 100).

49. As to claim 47, Studd teaches a method where the first processor is a client terminal and the second processor is embedded on a secure portable computing and data storage platform [404, fig. 4].

50. As to claim 48, Studd teaches a method where there are a plurality of first processors connected (i.e., multiple processors) via a client bridge to one or more second processor and arranged to implement different subsets of the processes in the task table of the second processor [par. 29, lines 7-11].

51. As to claim 49, Studd teaches a processing system comprising: a first processor in which is stored a first task table containing a plurality of process names and process identifiers, each associated with a process locator (i.e., Studd teaches a request for a list of mobile device application from mobile to device for which said mobile device application will be stored and executed [par. 51]);

a second processor in which is stored a second task table containing said process names with associated process identifiers (i.e., Studd teaches a mobile device containing list mobile device application [par. 51]);

the second processor including a distributed object execution manager for identifying a process to be executed and issuing a request to the first processor to execute said process (i.e., Studd teaches identifying a mobile application to execute [par. 51 - par. 53]);

and the first processor including a client distributed object execution manager for controlling the execution of said processes at the first processor, the results of execution of the processes implemented at the first processor being retumed to the second processor [par. 51 - par. 53].

Studd does not expressly teach:

wherein the operation being executed is a fingerprint- matching algorithm comprising a base minutiae finding process executed by the first processor and a minutiae matching process executed by the second processor, wherein the base minutiae finding process is a first stage of a biometric identity authentication process implemented between data derived from a user biometric parameter and an open portion of a biometric identification template to produce intermediate results,

said open portion is the portion containing data unauthorized modification of which may not cause an impostor to be incorrectly authenticated as a genuine user and comprises parameters of a predetermined number of unique features of the biometric identification template, and said intermediate results comprise parameters for alignment of said data and said biometric identification template and are transmitted from the first processor to the second processor, and wherein the minutiae matching process is a second stage of the biometric identity authentication process to issue a biometric authentication result using the intermediate results.

However, these features are well known in the art and would have been an obvious modification of the system disclosed by Studd as introduced by Hamid. Hamid discloses:

wherein the operation being executed is a fingerprint- matching algorithm comprising a base minutiae finding process executed by the first processor and a minutiae matching process executed by the second processor (to provide a fingerprint minutiae matching algorithm [col. 7, lines 20- 51]).

wherein the base minutiae finding process is a first stage of a biometric identity authentication process implemented between data derived from a user biometric parameter and an open portion of a biometric identification template to produce intermediate results (to provide a transmitting capability from a smart card a public portion (e.g., open) to a host computer for the purpose of authentication [par. 27],

said open portion is the portion containing data unauthorized modification of which may not cause an impostor to be incorrectly authenticated as a genuine user and comprises parameters of a predetermined number of unique features of the biometric identification template (to provide a public portion (e.g. open) containing authentication data [par. 27]),

and said intermediate results comprise parameters for alignment of said data and said biometric identification template and are transmitted from the first processor to the second processor, and wherein the minutiae matching process is a second stage of the biometric identity authentication process to issue a biometric authentication result using

the intermediate results (to provide processing at the host for biometric authentication [26, 27, fig. 3]].

Therefore, given the teachings of Hamid, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Studd by employing the well known features of a fingerprint matching algorithm disclosed above by Hamid, for which distributed authentication will be enhanced [col. 7, lines 20-51].

52. As to claim 50, Studd teaches a processing system where the first processor includes a client manager (i.e., input/output controller hub) for handling communications between the first and second processors (par. 31).

53. As to claim 51, Studd teaches a system where the first processor includes an execution manager (i.e., framework application services unit) for handling the execution of processes (i.e., mobile device application) [par. 51 - par. 53].

54. As to claim 52, Studd teaches a system where the first processor comprises a program store for holding said processes, the process locator (i.e., identifier) being used to identify the location of said processes in the program store [par. 51].

55. As to claim 53, Studd teaches a system where the second processor includes a remote device manager for transmitting said requests to the first processor [fig. 4].

56. As to claim 54, Studd teaches a system where the second processor comprises a stack for holding results returned to it from the first processor (par. 61).

57. As to claim 55, Studd teaches a system according where the second processor includes a program store for holding said processes (par. 51).

58. As to claim 56, Studd teaches a system where the first processor comprises a client terminal (fig. 4).

59. As to claim 57, Studd teaches a system which comprises a plurality of first processors, the system further comprising a client bridge (i.e., predetermine mechanism) for handling communications between the first processors and the second processor [par. 100].

60. As to claim 58, Studd teaches a system where each first processor comprises a server (par. 100, lines 6-9).

61. As to claim 59, Studd teaches a system where the client bridge includes a network execution manager (i.e., input/output controller hub) for transmitting requests

from the second processor to the appropriate one of the first processors, based on a processor identifier in the request [par. 31, lines 1-8].

62. As to claim 60, Studd teaches a system comprising a plurality of second processors and a client bridge (i.e., predetermine mechanism) for connecting said second processors to said first processor [par. 100, lines 1-9].

63. As to claim 61, Studd teaches a system where the second or each second processor is embedded on a respective portable secure computing and data storage platform such as smart card [par. 404, fig. 4].

Response to Arguments filed on 5/18/2009

Applicant's Remarks 102 Rejection Claims 1, 2, 3, 5, 7 through 25, 27 and 29

The Examiner contends Hamid specifically teaches a two stage biometric authentication between a smart card (e.g., user-presented) and host processor [figure 5]. Applicant argues, "The reconstructed portions of the image of the fingerprint can be modified by an imposter to cause an impostor to be incorrectly authenticated as a genuine user. Therefore, the public (e.g., open) portion in paragraphs 26- 27 of Hamid contains data unauthorized modification of which may cause an impostor to be incorrectly authenticated as a genuine user, in contrast to the open portion claimed in claim 1 of the present application which contains data unauthorized". Both Hamid and applicant teaches maintaining authentication data in the public portion (e.g., open portion) of a

system for authentication purposes. The Examiner contends speculating that one system data is maintained more securely than the other does not render sufficient basis for patentability. Examiner finds applicant's arguments non-persuasive.

With regards to applicant's remarks of the Hash value subject to be leaked [pg. 18], again the Examiner contends such remarks are speculative. Those skilled in the art would recognize the element of vulnerability within any communication system. Hamid's teaching of synchronization between devices is no less secure than applicant's teaching of client and host communication.

Applicant's Remarks 102 Rejection Claims 3, 5, and 7 through 23

The Examiner does not find applicant comments persuasive for claim 1. See Examiner remarks above. Therefore Examiner maintains present rejection for claims 3, 5, and 7-23 respectfully.

Applicant's Remarks 102 Rejection Claims 25, 27 and 29-37

The Examiner does not find applicant comments persuasive for claim 1. See Examiner remarks above. Therefore Examiner maintains present rejection for claims 25, 27 and 29-37 respectfully.

Applicant's Remarks 102 Rejection Claim 2

The Examiner contends Hamid teaches a two stage biometric authentication system. Further, Hamids teaches providing a public (e.g., open) portion from a smart card for

which is preprocessed registered biometric data [par. 26-27]. The Examiner contends applicant's "imposter" argument is speculative. Those skilled in the art would recognize the element of vulnerability within any communication system and that Hamid's teachings of synchronization between devices is no less secure then applicant's teaching of client and host communication. Therefore Examiner maintains present rejection for claim 2.

Applicant's Remarks 102 Rejection Claims 38 through 43 and 45 through 61

With regards to applicant's remarks on how Studd obtains processor information and that such a method would render the information vulnerable to leakage, the Examiner contends once Studd receives the processor information (e.g., application), it is then stored. It is common in the art to an download application to a mobile processor for the purpose of storing and executing the application on the processor. Applicant's arguments with respect to newly amended subject matter for claims 38-43 and 45-61 have been considered but are moot in view of the new ground(s) of rejection. The examiner contends Hamid teaches a two stage biometric authentication system utilizing a fingerprinting matching algorithm.

Contact Information

Any inquiry concerning this communication or earlier communications from the examiner should be directed to BRYAN WRIGHT whose telephone number is (571)270-3826. The examiner can normally be reached on 8:30 am - 5:30 pm Monday -Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William Korzuch can be reached on (571) 272-7589. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/BRYAN WRIGHT/
Examiner, Art Unit 2431

/William R. Korzuch/
Supervisory Patent Examiner, Art Unit 2431